IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
BILLINGS DIVISION

UNITED STATES OF AMERICA, **Plaintiff,** **vs.** **JOSE ANTONIO ESCOBEDO,** **Defendant.**	**CR 19-113-BLG-SPW** **ORDER DENYING DEFENDANT'S MOTION TO SUPPRESS**

The Government charges Defendant Jose Antonio Escobedo with conspiracy to possess with intent to distribute methamphetamine and possession with intent to distribute methamphetamine. (Doc. 7.) Before the Court is Escobedo's motion to suppress evidence. (Doc. 21.) The Government filed a response (Doc. 23), to which Escobedo filed a reply (Doc. 27). The Court held a hearing on the motion on November 8, 2019. For the following reasons, the Court denies Escobedo's motion to suppress.

I. Background

The Southwest Border Transaction Record Analysis Center (TRAC) is a web-accessible database law enforcement uses to monitor person-to-person money transfers concentrated in southwest border-states and Mexico. (Doc. 23 at 3.) It is

available online at www.sbtrac.com, but only law enforcement officers with a login and password may access it. (Doc. 27 at 2.)

In 2014, Western Union—a prominent person-to-person money transfer corporation—and the Arizona Attorney General entered into an agreement to create TRAC. (Doc. 23 at 3.) Western Union agreed to provide the Government with transaction data for all money transfers of $500 or more that are sent or received in California, Arizona, New Mexico, Texas, and Mexico. Since that time, several other money transfer services, like RIA Financial, have also agreed to provide the Government with the same data. The TRAC system now provides law enforcement with the information an individual supplies a third-party money transfer service to execute a money transfer, including the individual's name, address, date of birth, and other identifying information; the transaction date and amount; the location the funds were sent to; and the name of the transfer recipient. Law enforcement uses TRAC to investigate money laundering related to human trafficking, human smuggling, narcotics trafficking, and terrorism. Officers can search the database for transactions originating from particular cities over certain timeframes.

Sometime before August 2019, Border Patrol Agent Matt Henderson, who was assigned to the FBI Big Sky Transactional Organized Crime West Task Force (TFO Henderson), was monitoring TRAC for suspicious person-to-person transactions. (Doc. 23 at 2, 4.) He entered search criteria for recent money transfers

sent from Billings, Montana. (*Id.*) TRAC returned Escobedo's name in a series of money transfers sent to McAllen, Texas—a border city known for importing methamphetamine. TFO Henderson noted the frequency and amount sent were suspicious. He passed this information to Detective Tanner Buechler of the Eastern Montana High Intensity Drug Task Force. (*Id.* at 4.)

An investigation into Escobedo's criminal history showed he had been convicted for drug-related crimes in Texas. Therefore, Detective Beuchler began suspecting Escobedo was wiring money to McAllen in exchange for drugs sent through the mail. He identified Escobedo's physical address in Billings and contacted USPS Inspector Mike Smith. Inspector Smith discovered Escobedo had received several packages from McAllen, one of which was in USPS's possession and was scheduled to be delivered on August 12, 2019. (*Id.*) Investigators conducted a K9 sniff on the package, and the K9 alerted to the presence of narcotics. Inspector Smith obtained a search warrant based on this information and located 254.9 grams of a crystal substance later confirmed to be methamphetamine. Investigators replaced some of the substance with rock salt and prepared to conduct a controlled delivery. (*Id.*)

Detective Buechler obtained an anticipatory search warrant for Escobedo's home. (*Id.*) On August 13, 2019, task force officers conducted a controlled delivery.

(*Id.*) Escobedo retrieved the package and entered his home, after which officers executed the search warrant. (*Id.*)

On August 29, 2019, law enforcement served Custom Summonses on Western Union and RIA Financial—both services Escobedo had used to transfer money. (*Id.* at 5.) TFO Michael Robinson received the records on September 10, 2019. The records showed Escobedo sent money six times to McAllen, Texas, from May 7, 2019, to July 6, 2019. (*Id.*)

II. Discussion

Escobedo argues law enforcement improperly gathered the information about his money transfers. He argues he had an expectation of privacy in the information and law enforcement received it in violation of his rights under the Fourth Amendment. Therefore, evidence gathered as a result of examining data from the TRAC system must be suppressed.

Escobedo is incorrect; he did not have an expectation of privacy in the information. Western Union and RIA Financial—third parties—gave information about Escobedo's transactions to law enforcement. Escobedo lost any expectation of privacy he had in the information when he turned it over to the third parties. Moreover, it was non-content information—that is, the information did not contain the contents of a conversation or communication.

In *United States v. Miller*, 425 U.S. 435 (1976), after a fire broke out in Miller's warehouse, authorities discovered an underground distilling operation. *Id.* at 437. ATF agents then presented grand jury subpoenas to two banks Miller held accounts with and asked the banks to produce "all records of accounts, i.e., savings checking, loan or otherwise," in Miller's name. *Id.* The banks complied, but Miller moved to suppress the records as illegally seized. *Id.* at 439. The Supreme Court held Miller's bank records contained information he had voluntarily disclosed to the banks and their employees "in the ordinary course of business." *Id.* at 442. Therefore, Miller had no expectation of privacy in the records because "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection." *Id.* (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)). The Court continued,

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.
>
> *Id.* (internal citations removed).

In *Smith v. Maryland*, 442 U.S. 735, 737 (1979), a woman reported she was robbed by a man driving a 1975 Monte Carlo. After the robbery, the woman began receiving threatening phone calls from a man identifying himself as the robber. *Id.*

at 737. Police later spotted a man driving a 1975 Monte Carlo matching the robber's description. Using the vehicle's license plate, the police learned it was registered to the defendant, Smith. The next day, without a warrant or court order, officers installed a pen register at a telephone company to record numbers dialed from Smith's home. *Id.* That day, a call was placed to the victim. *Id.* On the basis of this and other evidence, officers received a search warrant for Smith's residence and ultimately arrested Smith for the robbery. Smith attempted to suppress evidence obtained from the pen register, and the issue reached the Supreme Court. *Id.*

The Supreme Court distinguished *Smith* from *Katz*, a case where the Court held unconstitutional the Government's warrantless use of a listening device to record a suspect's conversation in a phone booth. *Id.* at 741; *Katz*, 389 U.S. at 353. *Smith* differed because unlike the listening device employed in *Katz*, "pen registers do not acquire the *contents* of communications." *Smith*, 442 U.S. at 741 (emphasis in original). Instead, pen registers only disclosed phone numbers that were dialed. *Id.* "Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." *Id.* (quoting *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977)). So, the Supreme Court rejected Smith's claim and determined telephone users have no subjective expectation of privacy in the numbers they dial because they know telephone companies record the numbers. *Id.* at 743. Moreover, such an

expectation of privacy would be unreasonable: "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743–44. In other words, when Smith "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business," he "assumed the risk that the company would reveal to police the numbers he dialed." *Id.* at 744.

More recently, the Ninth Circuit affirmed a case with similar facts to Escobedo's in *United States v. Cormier*, 220 F.3d 1103 (9th Cir. 2000). There, a detective went to a motel located in a traditionally high-crime area to obtain the motel's guest registration records. After the motel voluntarily turned over the records, the detective ran a criminal record check on several guests, including Cormier. The check revealed Cormier had an extensive criminal history and was registered as a sex offender. A second detective then conducted a "knock and talk" interview with Cormier in his motel room that eventually led the detective to discover Cormier unlawfully possessed a firearm. *Id.* at 1106. The Ninth Circuit affirmed the first detective's examination of the motel's guest registry, even though the first detective had not been investigating Cormier before seeing his name in the records. *Id.* at 1108. Looking to *Miller* for guidance, the Circuit found the third party—the motel—had turned over the guest registry voluntarily and the records only contained Cormier's name and room number. *Id.* Therefore, the Circuit held

Cormier did not have a reasonable expectation of privacy in the registration records. *Id.*

But *Miller*, *Smith*, and *Cormier* are not without their limits, and giving information to third parties does not always grant the Government unfettered access to it. The Supreme Court recently drew the line when cell phone location information is involved. *Carpenter v. U.S.*, 138 S. Ct. 2206, 2216 (2018). Although a cell phone user may give location data to a wireless carrier when using the carrier's service, the location information is "detailed, encyclopedic, and effortlessly compiled." *Id.* at 2216. In such circumstances, the Court declined to extend *Smith* and *Miller*:

> Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in *Jones*[1] or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell-site location information]. The location information obtained from Carpenter's wireless carriers was the product of a search.

Id. at 2217.

The above cases illustrate how Escobedo did not have an expectation of privacy in the non-content information he turned over to Western Union and RIA

[1] *United States v. Jones*, 565 U.S. 400 (2012): long-term GPS monitoring of a vehicle impinges on expectations of privacy, regardless whether those movements are disclosed to the public at-large.

Financial. Escobedo provided information to Western Union and RIA Financial to transfer funds from Billings, Montana, to McAllen, Texas. Both companies sent data regarding the transactions to TRAC. Law enforcement did not require a warrant before inspecting the TRAC data. This is because Escobedo "voluntarily conveyed" his transactional information to the money services companies and "'exposed' that information to [their] equipment in the ordinary course of business." *Smith*, 422 U.S. at 744. Therefore, Escobedo "assumed the risk that the company[ies] would reveal to police" the information he provided. *Id.* Whether the third parties gave law enforcement the information voluntarily or pursuant to a subpoena is irrelevant: Escobedo lost any expectation of privacy he had in the information when he voluntarily conveyed it to Western Union and RIA Financial.

First, the data does not contain the contents of any communications. Escobedo argues the information "goes beyond non-content information provided to a third party." (Doc. 27 at 3.) But *Smith* distinguished a pen registry, which records only phone numbers (non-content information), from the listening device in *Katz*, which allowed the Government to listen to and record the *contents* of a communication. *Smith* 442 U.S. at 741. Escobedo voluntarily conveyed information identifying himself, the name and location of his recipient, and the amount sent to both Western Union and RIA Financial. The information did not contain the content of any communication Escobedo had with his intended recipients. Escobedo

assumed the risk that both companies would provide such non-content information to law enforcement through the TRAC system.

Second, *Cormier* establishes law enforcement may begin an investigation into criminal activity by examining third party information, even if officers do not have a particular target or suspect in mind when examining it. *Cormier*, 220 F.3d at 1107–08. The motel registration records in *Cormier* informed officers of each guest's name, room number, and the fact that the guest was residing at the motel. *Id.* Before examining the motel records, the only suspicion officers had was that the motel was in a high-crime area. *Id.* at 1106. The money transfer information at issue here allowed officers to identify Escobedo, the name and location of his recipient, and the fact that Escobedo was sending large sums of money to McAllen, Texas. Before examining the TRAC records, the only suspicion officers had was that large money transfers sent to border states could indicate narcotics trafficking. However, like the defendant in *Cormier*, Escobedo had no reasonable expectation of privacy in the records after he voluntarily conveyed the information to third parties.

Third, *Carpenter* is useful to illustrate the limitations of *Miller* and *Smith*. *Carpenter* shows there is a point where a third party can have such "detailed, encyclopedic, and effortlessly compiled" information about an individual that Government access to the information constitutes a search under the Fourth Amendment. *Carpenter*, 138 S. Ct. at 2216–17. This applies to detailed information

about an individual's location and movements: "Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection." *Id.* at 2217. Escobedo's money transfer information, however, does not rise to the level of the detailed, encyclopedic, and effortlessly compiled location information in *Carpenter*. The Western Union records gave the Government information about six money transfers Escobedo sent to McAllen, Texas. Even if the information contained identifying information about Escobedo, the location he sent the money, the name of its recipient, and the amount transferred, the data did not paint a precise picture of Escobedo's movements over a given time like the cell phone location information from *Carpenter*.

Finally, Escobedo briefly mentions the Right to Financial Privacy Act of 1978 in his brief. Escobedo correctly points out the Act, which was Congress's response to *Miller*, prohibits financial institutions from providing the Government with financial information without certain express authorizations. 12 U.S.C. §§ 3401–22. However, even if the Act applied here, there is no right to suppress evidence under it. Remedies for violations are only civil in nature. *United States v. Frazin*, 780 F.2d 1461, 1464 (9th Cir. 1986).

III. Conclusion

The Government's use of the TRAC system to find and monitor Escobedo's transactions is permissible under the Fourth Amendment. The information Western Union and RIA Financial provided to the TRAC system did not contain the content of Escobedo's conversations or communications. It was permissible for law enforcement to initiate an investigation by examining the records, even if officers did not have a target or suspect in mind before reviewing them. Finally, the information about Escobedo's six money transfers did not contain precise details about his movements like cell service location information would, nor was it detailed, encyclopedic, and effortlessly compiled. Accordingly,

IT IS HEREBY ORDERED Escobedo's Motion to Suppress Evidence (Doc. 21) is **DENIED**.

Dated this 2nd day of ~~November~~ December, 2019.

SUSAN P. WATTERS
United States District Court Judge